

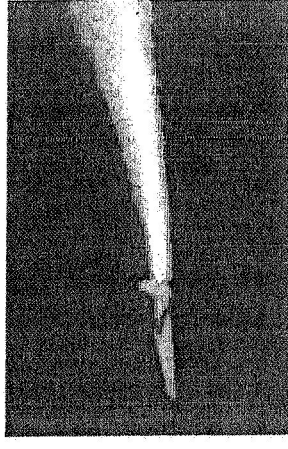
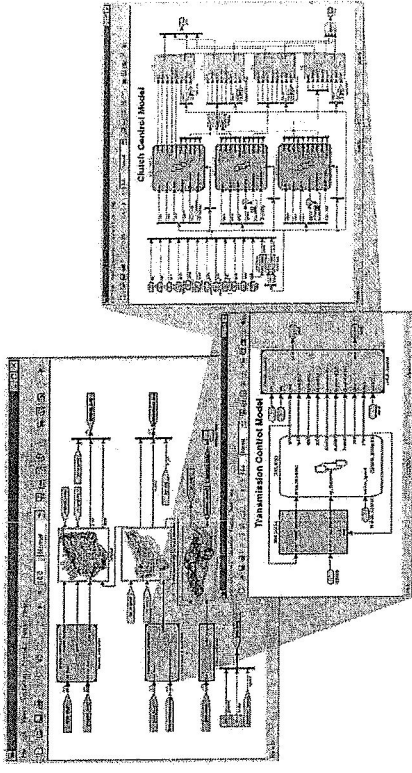
A Software Safety Certification Plug-in for Automated Code Generators (Executive Briefing)

PI: Ewen Denney, USRA/RIACS
Johann Schumann, USRA/RIACS
Doug Greaves, NASA Ames

Auto-generated code at NASA

- c.50% of NASA missions and projects use modeling tools like Simulink and Matlab
- Commercial code generators (e.g., Real-Time Workshop and MatrixX) are available and have been successfully used
 - X-43 Hyper-X: On-board flight-software generated from Simulink models
 - RASCAL: Helicopter control laws implemented using Real-Time Workshop

"We never found any errors in the automatically generated code, so we were confident in creating a quick prototype for NASA." (P. Seigman, Boeing)



Safety of auto-generated code

- “Experience shows everything is fine...”
- A look into RT Workshop shows:

/* Copyright 1994-2002 The MathWorks, Inc.

```
...
for (;;) {
    utAssert( (x[bottom] < u) && (u < x[top]) );
    idx = (bottom + top)/2;
    if (u < x[idx]) { top = idx - 1;
    } else if (u >= x[idx+1]) {
        bottom = idx + 1;
    } else { return(idx);
    }
}
```

Code used for Simulink
table interpolation

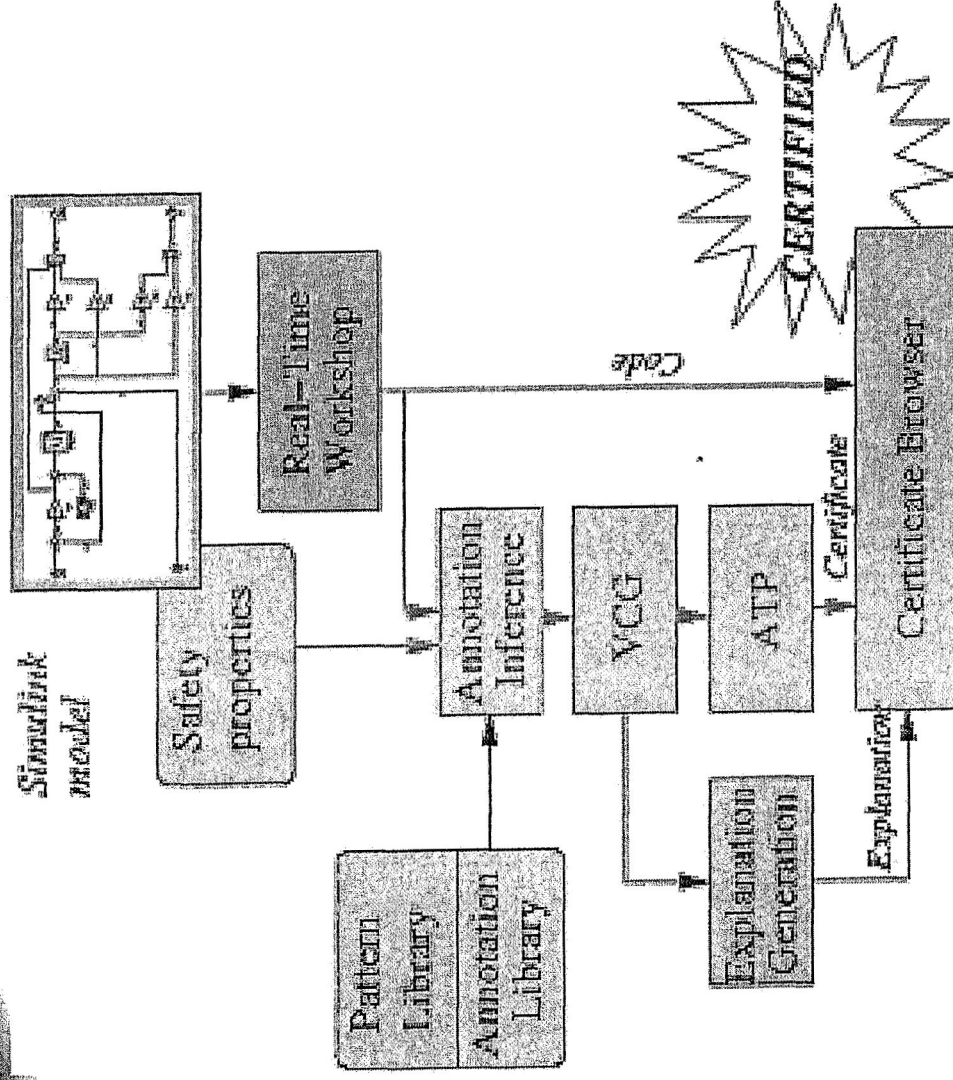
*Assertion does not
match with program.
If activated, can lead
to program abort*

For safety-critical and human-rated applications, good
experience is not enough. IV&V needs formal tools to check

safety of auto-generated code

Technical approach

- Combine generator with certification tool
- Generate certificates which can be verified independently (IV&V)
- Based on formal logic
 - Range of safety properties
 - Pattern-based approach to inferring annotations
 - Fully automated



Audit support

- Display and explanation of proof tasks

- explain *why* code is safe

- “the table lookup, `fl[b+i]`, at line 23, is within bounds because ...”
=> support code reviews

- Traceability to code (and model...)

Proof
Status

The screenshot shows a code editor with C code for quaternion operations. Annotations include arrows pointing to specific code lines and a table of verification conditions.

Show obligations (points to line 213)

Highlight code (points to line 213)

Formula or explanation (points to line 213)

Safety Obligations (points to line 213)

Verification Conditions

Condition	Proof Status
<code>quaternion_dsl_init_0024</code>	PROVEN
<code>quaternion_dsl_init_0025</code>	PROVEN
<code>quaternion_dsl_init_0026</code>	PROVEN
<code>quaternion_dsl_init_0027</code>	PROVEN
<code>quaternion_dsl_init_0028</code>	PROVEN
<code>quaternion_dsl_init_0029</code>	PROVEN
<code>quaternion_dsl_init_0030</code>	PROVEN
<code>quaternion_dsl_init_0031</code>	PROVEN
<code>quaternion_dsl_init_0032</code>	PROVEN
<code>quaternion_dsl_init_0033</code>	PROVEN
<code>quaternion_dsl_init_0034</code>	PROVEN
<code>quaternion_dsl_init_0035</code>	PROVEN
<code>quaternion_dsl_init_0036</code>	PROVEN
<code>quaternion_dsl_init_0037</code>	PROVEN
<code>quaternion_dsl_init_0038</code>	PROVEN
<code>quaternion_dsl_init_0039</code>	PROVEN
<code>quaternion_dsl_init_0040</code>	PROVEN
<code>quaternion_dsl_init_0041</code>	PROVEN
<code>quaternion_dsl_init_0042</code>	PROVEN
<code>quaternion_dsl_init_0043</code>	PROVEN
<code>quaternion_dsl_init_0044</code>	PROVEN
<code>quaternion_dsl_init_0045</code>	PROVEN
<code>quaternion_dsl_init_0046</code>	PROVEN
<code>quaternion_dsl_init_0047</code>	PROVEN
<code>quaternion_dsl_init_0048</code>	PROVEN
<code>quaternion_dsl_init_0049</code>	PROVEN
<code>quaternion_dsl_init_0050</code>	PROVEN
<code>quaternion_dsl_init_0051</code>	PROVEN
<code>quaternion_dsl_init_0052</code>	PROVEN
<code>quaternion_dsl_init_0053</code>	PROVEN
<code>quaternion_dsl_init_0054</code>	PROVEN
<code>quaternion_dsl_init_0055</code>	PROVEN
<code>quaternion_dsl_init_0056</code>	PROVEN
<code>quaternion_dsl_init_0057</code>	PROVEN
<code>quaternion_dsl_init_0058</code>	PROVEN
<code>quaternion_dsl_init_0059</code>	PROVEN
<code>quaternion_dsl_init_0060</code>	PROVEN
<code>quaternion_dsl_init_0061</code>	PROVEN
<code>quaternion_dsl_init_0062</code>	PROVEN
<code>quaternion_dsl_init_0063</code>	PROVEN
<code>quaternion_dsl_init_0064</code>	PROVEN
<code>quaternion_dsl_init_0065</code>	PROVEN
<code>quaternion_dsl_init_0066</code>	PROVEN
<code>quaternion_dsl_init_0067</code>	PROVEN
<code>quaternion_dsl_init_0068</code>	PROVEN
<code>quaternion_dsl_init_0069</code>	PROVEN
<code>quaternion_dsl_init_0070</code>	PROVEN
<code>quaternion_dsl_init_0071</code>	PROVEN
<code>quaternion_dsl_init_0072</code>	PROVEN
<code>quaternion_dsl_init_0073</code>	PROVEN
<code>quaternion_dsl_init_0074</code>	PROVEN
<code>quaternion_dsl_init_0075</code>	PROVEN
<code>quaternion_dsl_init_0076</code>	PROVEN
<code>quaternion_dsl_init_0077</code>	PROVEN
<code>quaternion_dsl_init_0078</code>	PROVEN
<code>quaternion_dsl_init_0079</code>	PROVEN
<code>quaternion_dsl_init_0080</code>	PROVEN
<code>quaternion_dsl_init_0081</code>	PROVEN
<code>quaternion_dsl_init_0082</code>	PROVEN
<code>quaternion_dsl_init_0083</code>	PROVEN
<code>quaternion_dsl_init_0084</code>	PROVEN
<code>quaternion_dsl_init_0085</code>	PROVEN
<code>quaternion_dsl_init_0086</code>	PROVEN
<code>quaternion_dsl_init_0087</code>	PROVEN
<code>quaternion_dsl_init_0088</code>	PROVEN
<code>quaternion_dsl_init_0089</code>	PROVEN
<code>quaternion_dsl_init_0090</code>	PROVEN
<code>quaternion_dsl_init_0091</code>	PROVEN
<code>quaternion_dsl_init_0092</code>	PROVEN
<code>quaternion_dsl_init_0093</code>	PROVEN
<code>quaternion_dsl_init_0094</code>	PROVEN
<code>quaternion_dsl_init_0095</code>	PROVEN
<code>quaternion_dsl_init_0096</code>	PROVEN
<code>quaternion_dsl_init_0097</code>	PROVEN
<code>quaternion_dsl_init_0098</code>	PROVEN
<code>quaternion_dsl_init_0099</code>	PROVEN
<code>quaternion_dsl_init_0100</code>	PROVEN

Auto-generated code

USRA - RESEARCH INSTITUTE FOR ADVANCED COMPUTER SCIENCE



Project plan

- Phase I (6 months)
 - Determine how certification machinery must be adapted for Real-Time Workshop
 - Demonstrate fully automated verification on useful subset of Simulink blocks for limited range of policies on selected examples
- Phase II
 - Extend and mature prototype
 - Deliverable: Cert/RT – certification tool for RTW
 - Further case studies